

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Toshiharu TAKEMURA, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: DATA COMMUNICATION APPARATUS AND METHOD FOR MANAGING MEMORY IN THE SAME

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. _____ Date Filed _____
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

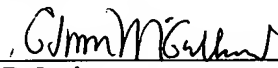
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-104706	April 9, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. _____ filed _____
- ☐ were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____; and
- ☐ (B) Application Serial No.(s) _____
☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle

Registration No. 40,073

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

C. Irvin McClelland
Registration Number 21,124



日 本 国 特 許 庁
JAPAN PATENT OFFICE

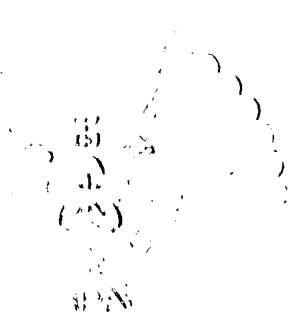
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 4 月 9 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 0 4 7 0 6
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 1 0 4 7 0 6]

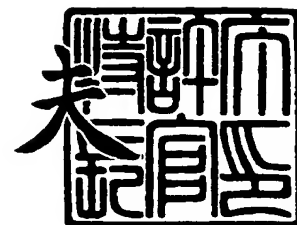
出 願 人 ソニー株式会社
Applicant(s):




2 0 0 4 年 2 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫





【書類名】 特許願

【整理番号】 0290783002

【提出日】 平成15年 4月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G06K 19/07

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 竹村 俊治

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 森田 直

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 久保野 文夫

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 栗田 太郎

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 市川 琢也

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

【選任した代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【手数料の表示】

【予納台帳番号】 048747

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記憶媒体及び情報記憶媒体のメモリ管理方法

【特許請求の範囲】

【請求項 1】

メモリ空間と、

前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義手段と、

サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義手段と、
を具備することを特徴とする情報記憶媒体。

【請求項 2】

前記メモリ空間上に設けられた 1 以上のサービス・メモリ領域を含むエリアを定義するエリア定義手段をさらに備える、
ことを特徴とする請求項 1 に記載の情報記憶媒体。

【請求項 3】

前記暗証コード・サービス定義手段は、エリア内にアクセスする前に暗証コード照合処理を行なう暗証コード・サービスを定義する、
ことを特徴とする請求項 2 に記載の情報記憶媒体。

【請求項 4】

前記サービス定義手段により既に設けられているサービス・メモリ領域に対して適用する他のサービスを重複して定義するオーバーラップ・サービス定義手段をさらに備える、
ことを特徴とする請求項 1 に記載の情報記憶媒体。

【請求項 5】

前記暗証コード・サービス定義手段は、前記重複して定義された他のサービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する、
ことを特徴とする請求項 4 に記載の情報記憶媒体。

【請求項 6】

前記暗証コード・サービスによる暗証コード照合処理を有効又は無効に設定す

る照合処理制御手段をさらに含む、
ことを特徴とする請求項 1 に記載の情報記憶媒体。

【請求項 7】

メモリ空間を備えた情報記憶媒体におけるメモリ管理方法であって、
前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義ステップと、
サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義ステップと、
を具備することを特徴とする情報記憶媒体のメモリ管理方法。

【請求項 8】

前記メモリ空間上に設けられた 1 以上のサービス・メモリ領域を含むエリアを定義するエリア定義ステップをさらに備える、
ことを特徴とする請求項 7 に記載の情報記憶媒体のメモリ管理方法。

【請求項 9】

前記暗証コード・サービス定義ステップでは、エリア内にアクセスする前に暗証コード照合処理を行なう暗証コード・サービスを定義する、
ことを特徴とする請求項 8 に記載の情報記憶媒体のメモリ管理方法。

【請求項 10】

前記サービス定義ステップにより既に設けられているサービス・メモリ領域に対して適用する他のサービスを重複して定義するオーバーラップ・サービス定義ステップをさらに備える、
ことを特徴とする請求項 7 に記載の情報記憶媒体のメモリ管理方法。

【請求項 11】

前記暗証コード・サービス定義ステップでは、前記重複して定義された他のサービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する、
ことを特徴とする請求項 10 に記載の情報記憶媒体のメモリ管理方法。

【請求項 12】

前記暗証コード・サービスによる暗証コード照合処理を有効又は無効に設定す

る照合処理制御ステップをさらに含む、
ことを特徴とする請求項 7 に記載の情報記憶媒体のメモリ管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、比較的大容量のメモリ領域を備えた情報記憶媒体及び情報記憶媒体のメモリ管理方法に係り、特に、メモリ領域上に 1 以上のアプリケーションが割り当てられた情報記憶媒体及び情報記憶媒体のメモリ管理方法に関する。

【0002】

さらに詳しくは、本発明は、メモリ領域上に割り当てられているアプリケーション毎にアクセスを管理・制限する情報記憶媒体及び情報記憶媒体のメモリ管理方法に係り、特に、アプリケーションに割り当てられている個々のサービス・メモリ領域に対して複数のアクセス方法を提供する情報記憶媒体及び情報記憶媒体のメモリ管理方法に関する。

【0003】

【従来の技術】


局所でのみ適用可能な無線通信手段の一例として、非接触 IC カードを挙げることができる。

【0004】

この種の無線通信には、一般に、電磁誘導の原理に基づいて実現される。すなわち、メモリ機能を有する IC カードと、IC カードのメモリに対して読み書きアクセスをするカード・リーダ／ライタで構成され、1 次コイルとしての IC カード側のループ・コイルと 2 次コイルとしてのカード・リーダ／ライタ側のアンテナが系として 1 個のトランスを形成している。そして、カード・リーダ／ライタ側から IC カードに対して、電力と情報を同じく電磁誘導作用により伝送し、IC カード側では供給された電力によって駆動してカード・リーダ／ライタ側からの質問信号に対して応答することができる。

【0005】

カード・リーダ／ライタ側では、アンテナに流す電流を変調することで、IC



カード上のループ・コイルの誘起電圧が変調を受けるという作用により、カード・リーダ／ライタから I C カードへのデータ送信を行なうことができる。また、I C カードは、ループ・コイルの端子間の負荷変動により、I C カード・リーダ／ライタ側のアンテナ端子間のインピーダンスが変化してアンテナの通過電流や電圧が変動するという作用により、カード・リーダ／ライタへの返信を行なう。

【0006】

I C カードに代表される非接触・近接通信システムは、操作上の手軽さから、広範に普及している。例えば、暗証コードやその他の個人認証情報、電子チケットなどの価値情報などを I C カードに格納しておくことにより、キャッシュ・ディスプレイやコンサート会場の出入口、駅の改札口などに設置されたカード・リーダ／ライタは、利用者がかざした I C カードに非接触でアクセスして、認証処理を行なうことができる。

【0007】

最近では、微細化技術の向上とも相俟って、比較的大容量のメモリ空間を持つ I C カードが出現している。大容量メモリ付きの I C カードによれば、複数のアプリケーションを同時に格納しておくことができるので、1枚の I C カードを複数の用途に利用することができる。例えば、1枚の I C カード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、多数のアプリケーションを格納しておくことにより、1枚の I C カードをさまざまな用途に適用させることができる。ここで言う電子マネーや電子チケットは、利用者が提供する資金に応じて発行される電子データを通じて決済（電子決済）される仕組み、又はこのような電子データ自体を指す。

【0008】

さらに、I C カードやカード用リーダ／ライタ（カード読み書き装置）が無線・非接触インターフェースの他に、外部機器と接続するための有線インターフェース（図示しない）を備えることにより、I C カードやリーダ／ライタ機能を携帯電話機、PDA（Personal Digital Assistant）やパーソナル・コンピュータなどの各デバイスに I C カード及びカード・リーダ／ライタのいずれか一方又は双方の機能を装備することができる。

【0009】

このような場合、ICカード技術を汎用性のある双方向の近接通信インターフェースとして利用することができる。例えば、コンピュータや情報家電機器のような機器同士で近接通信システムが構成される場合には、通信は一対一で行なわれる。また、ある機器が非接触ICカードのような機器以外の相手デバイスと通信することも可能であり、この場合においては、1つの機器と複数のカードにおける一対多の通信を行なうアプリケーションも考えられる。

【0010】


また、電子決済を始めとする外部との電子的な価値情報のやり取りなど、ICカードを利用したさまざまなアプリケーションを、情報処理端末上で実行することができる。例えば、情報処理端末上のキーボードやディスプレイなどのユーザ・インターフェースを用いてICカードに対するユーザ・インタラクションを情報処理端末上で行なうことができる。また、ICカードが携帯電話機と接続されていることにより、ICカード内に記憶された内容を電話網経由でやり取りすることもできる。さらに、携帯電話機からインターネット接続して利用代金をICカードで支払うことができる。

【0011】

ICカードの一般的な使用方法は、利用者がICカードをカード・リーダ／ライタをかざすことによって行なわれる。カード・リーダ／ライタ側では常にICカードをポーリングしており外部のICカードを発見することにより、両者間の通信動作が開始する。

【0012】

このとき、利用者が暗証番号をICカード・リーダ側に入力して、入力された暗証番号をICカード上に格納された暗証番号と照合することで、ICカードとICカード・リーダ／ライタ間で本人確認又は認証処理が行なわれる。(ICカード・アクセス時に使用する暗証番号のことを、特にPIN(Personal Identification Number)と呼ぶ。)そして、本人確認又は認証処理に成功した場合には、例えば、ICカード内に保存されているアプリケーションの利用、すなわち、アプリケーションに割り当てられているサービス・メモリ領域へのアクセスが可



能となる（本明細書中では、アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ）。サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

【0013】

本明細書中では、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

【0014】

上述したように単一のICカードが複数のアプリケーションに利用されている場合、アプリケーション毎にアクセス権を制御する必要があることから、アプリケーション毎に暗証コードを割り当てて、アプリケーション単位で照合処理してアクセスを制御することが一般的である。

【0015】

他方、アプリケーションに対して適用することができるサービスの種類は、個々のアプリケーションが持つ性質や必要とされるセキュリティ・レベルなどの属性情報に応じて区々であるが、これ以外にも、アプリケーションの利用者毎に割り当てられているアクセス権限に応じてサービス内容を制御したいという要請がある。例えば、ユーザAにはサービス・メモリ領域へのフルアクセスを許容してもよいが、他のユーザBには読み出し動作しか認められない場合など、ユーザ間で差別化を図りたいである。

【0016】

ところが、単にアプリケーションに暗証コードを割り当ててアクセスを制御するという方法では、暗証コードによって一旦照合処理を通過してしまうと、誰もがアプリケーションが定義しているサービスを一様に利用可能となる。言い換えれば、ユーザ毎にアプリケーション利用の権限を変えて、差別化を図るような場合（ユーザによって、サービス・メモリ領域への読み出し／書き込みを含んだサービスの利用を許容したり、読み出しのみのサービスの利用のみとしたりする）

であっても、すべてのユーザに対して一様なサービスを提供してしまうことになる。

【0017】

【発明が解決しようとする課題】

本発明の目的は、メモリ領域上に1以上のアプリケーションが割り当てられた情報記憶媒体において、アプリケーションに割り当てられている個々のサービス・メモリ領域に対して、ユーザ毎に異なるアクセス権限を与え、複数のアクセス方法を提供することができる、優れた情報記憶媒体及び情報記憶媒体のメモリ管理方法を提供することにある。

【0018】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第1の側面は、メモリ空間と、

前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義手段と、

サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義手段と、
を具備することを特徴とする情報記憶媒体である。

【0019】

また、本発明の第2の側面は、メモリ空間を備えた情報記憶媒体におけるメモリ管理方法であって、

前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義ステップと、

サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義ステップと、
を具備することを特徴とする情報記憶媒体のメモリ管理方法である。

【0020】

ここで言う情報記憶媒体とは、例えば、電磁誘導の原理に基づく非接触・無線通信インターフェースを備えたICカードなどであり、ICカード内には比較的

大容量のメモリが内蔵されている。

【0021】

本発明によれば、メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義し、さらにサービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義することにより、ICカードのセキュアな利用を確保することができる。

【0022】

メモリ空間上に設けられた1以上のサービス・メモリ領域を含むエリアを定義することができる。また、エリア内にアクセスする前に暗証コード照合処理を行なう暗証コード・サービスを定義するようにしてもよい。

【0023】

サービス・メモリ領域毎に暗証コードを設定できる以外に、各エリアに対しても暗証コードを設定することができるので、メモリ領域へのアクセス権を階層的に制御することができる。また、複数のサービスに対して共通の暗証コードを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。

【0024】

例えば、あるエリアに該当する暗証コードを入力することにより、照合・認証処理を経て、エリア内のすべてのサービス・メモリ領域（並びにサブエリア）へのアクセス権を与えるようにすることもできる。したがって、例えば、該当するエリアに対する暗証コードの入力を1回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。

【0025】

また、既に設けられているサービス・メモリ領域に対して適用する他のサービスを重複して定義する、すなわちオーバーラップ・サービスを定義するようにしてもよい。

【0026】

オーバーラップ・サービスを定義することにより、あるサービス・メモリ領域

に対して、「読み出しのみ」、「読み出し及び書き込み」など複数のアクセス方法を設定することができる。

【0027】

また、オーバーラップ・サービス定義を行なう場合、サービス毎に暗証コードを設定するようにしてもよい。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々の暗証コードが設定される。また、あるメモリ領域に対する読み出しについては暗証コードの入力が必要でないが、書き込む場合には暗証コードの入力を必須とさせることが可能である。

【0028】

また、暗証コード・サービスによる暗証コード照合処理を有効又は無効に設定する照合処理の制御を行なうようにしてもよい。

【0029】

サービス又はエリアに対する暗証コード・サービスが有効になっている場合にのみ、サービスの起動又はエリアへのアクセスを行なう前に暗証コードの照合が要求され、暗証コード・サービスが無効にされている場合には暗証コードの照合は要求されない。

【0030】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0031】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態について詳解する。

【0032】

A. 非接触通信システム

本発明は、ICカードを利用した非接触データ通信システムに関するものである。この種の非接触データ通信システムは、一般に、電磁誘導の原理に基づいて実現される。すなわち、メモリ機能を有するICカードと、ICカードのメモリ

に対して読み書きアクセスをするカード・リーダ／ライタで構成され、1次コイルとしてのICカード側のループ・コイルと2次コイルとしてのカード・リーダ／ライタ側のアンテナが系として1個のトランスを形成している。カード・リーダ／ライタ側からICカードに対して、電力と情報を同じく電磁誘導作用により質問信号を伝送する。そして、ICカード側では供給された電力によって駆動し、質問信号に対する応答信号に応じて自身のアンテナ間の負荷を変化させることによって読み書き装置の受信回路に現れる信号に振幅変調をかけて通信を行なう。なお、以下の説明では、携帯端末などに内蔵して使用されるICチップも含めて、「ICカード」と呼ぶことにする。

【0033】

図1には、電磁誘導に基づくリーダ／ライタ101とICカード50との無線通信の仕組みを概念的に図解している。リーダ／ライタ101は、ループ・コイルで構成されたアンテナ L_{RW} を備え、このアンテナ L_{RW} に電流 I_{RW} を流すことでその周辺に磁界を発生させる。一方、ICカード50側では、電気的にはICカード50の周辺にループ・コイル L_c が形成されている。ICカード50側のループ・コイル L_c 端にはリーダ／ライタ101側のループ・アンテナ L_c が発する磁界による誘導電圧が生じ、ループ・コイル L_c 端に接続されたICカード50の端子に入力される。

【0034】

リーダ／ライタ101側のアンテナ L_{RW} とICカード50側のループ・コイル L_c は、その結合度は互いの位置関係によって変わるが、系としては1個のトランスを形成していると捉えることができ、図2に示すようにモデル化することができる。

【0035】

リーダ／ライタ101は、アンテナ L_{RW} に流す電流 I_{RW} を変調することで、ICカード上のループ・コイル L_c に誘起される電圧 V_0 は変調を受け、そのことを利用してリーダ／ライタ101はICカード50へのデータ送信を行なうことができる。ここで言う送信データには、リーダ／ライタ101に接続された外部機器側でユーザ入力された暗証番号やパスワードなどの、アプリケーションやエリ

アへのアクセス権を得るための暗証コードや、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【0036】

また、ICカード50は、リーダ/ライタ101へ返送するためのデータに応じてループ・コイル L_c の端子間の負荷を変動させる機能 (Load Switching) を持つ。ループ・コイル L_c の端子間の負荷が変動すると、リーダ/ライタ101側ではアンテナ端子間のインピーダンスが変化して、アンテナ L_{RW} の通過電流 I_{RW} や電圧 V_{RW} の変動となって現れる。この変動分を復調することで、リーダ/ライタ101はICカード50の返送データを受信することができる。リーダ/ライタ101がICカード50から受信するデータには、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【0037】

B. ICカード内のメモリ空間の構造

携帯端末10に内蔵されたICカード50内のメモリには、電子決済を始めとする外部との電子的な価値情報のやり取りなど、1以上のアプリケーションが割り当てられている。アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ。また、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

【0038】

ユーザがアクセス権を持つかどうかに応じてアプリケーションの利用すなわちサービスの起動を制限するために、アプリケーションに対して暗証コードを割り当て、サービス実行時に暗証コードの照合処理を行なうようになっている。また、サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

【0039】

本実施形態では、ICカード50内のメモリ空間に対して、「ディレクトリ」に類似する階層構造を導入する。そして、メモリ領域に割り当てられた各アプリ

ケーションを、所望の階層の「エリア」に登録することができる。例えば、一連のトランザクションに使用される複数のアプリケーション、あるいは関連性の深いアプリケーション同士を同じエリア内のサービス・メモリ領域登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことによって、メモリ領域のアプリケーションやエリアの配置が整然とし、ユーザにとってはアプリケーションの分類・整理が効率化する。

【0040】

また、メモリ領域へのアクセス権を階層的に制御するために、アプリケーション毎に暗証コードを設定できる以外に、各エリアに対しても暗証コードを設定することができるようにした。例えば、あるエリアに該当する暗証コードを入力することにより、照合・認証処理を経て、エリア内のすべてのアプリケーション（並びにサブエリア）へのアクセス権を与えるようにすることもできる。したがって、例えば、該当するエリアに対する暗証コードの入力を1回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。

【0041】

さらに、本実施形態において特徴的なのは、あるサービス・メモリ領域に対するアクセス権限が単一でないことを許容し、それぞれのアクセス権限毎、すなわちサービス・メモリ領域において実行するサービスの内容毎に、暗証コードを設定することができるという点である。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々の暗証コードが設定される。また、あるメモリ領域に対する読み出しについては暗証コードの入力が必要でないが、書き込む場合には暗証コードの入力を必須とさせることが可能である。適用するサービス毎に暗証コードを設定する点については、後に詳解する。

【0042】

図3には、本実施形態に係るICカード50内の機能構成を図解している。同

図に示すように、ICカード50は、リーダ／ライタ101と無線通信を行なうアンテナが接続されるRF部51と、アプリケーション毎に割り当てられたサービス・メモリ領域を持つメモリ52（前述）と、RF部51などから入力された暗証コードの比較照合を行なう照合部53と、これらの構成部品を統括的にコントロールする制御部55とからなる。

【0043】

制御部55は、CPU（Central Processing Unit）、ROM（Read Only Memory）、RAM（Random Access Memory）などを一体化して構成されている。制御部55は、ROMに格納されたプログラム・コードを実行することによって、ICカード50内の動作を制御する。

【0044】

メモリ52は、1以上のアプリケーションに対して記憶領域を割り当てるために使用される。メモリ52は、半導体メモリの他、磁気ストライプなど、読み書き可能な記憶媒体であればよく、特定のデバイスには限定されない。

【0045】

本実施形態では、メモリ52が持つ記憶空間には、「ディレクトリ」に類似する階層構造が導入されている。すなわち、メモリ領域に割り当てられた各アプリケーションを、所望の階層エリアにサービス・メモリ領域として登録することができる。例えば、一連のトランザクションに使用されるアプリケーションなど、関連性の深いアプリケーション同士を同じエリアに登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことができる。

【0046】

また、メモリ52内に割り当てられたアプリケーション（すなわちサービス・メモリ領域）並びにエリアは暗証コード定義ブロックを備えている。したがって、アプリケーション毎に、あるいはエリア毎に暗証コードを設定することができる。また、メモリ52に対するアクセス権は、アプリケーション単位で行なうとともに、並びにエリア単位で行なうことができる。

【0047】

さらに、あるサービス・メモリ領域に対するアクセス権限が単一でなく、実行

するサービスの内容毎に、暗証コードを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定され、また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々の暗証コードが設定される（後述）。

【0048】

照合部53は、例えばRF部51を介して送られてくる暗証コードを、各アプリケーション又はディレクトリに割り当てられたエリア又はサービス・メモリ領域に設定されている暗証コードと照合して、一致するメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、RF部51を介してリーダー/ライター101から読み書きが可能となる。

【0049】

C. 暗証コードの適用

上述したようにICカード内のメモリには、アプリケーションに割り当てられたさまざまなサービス・メモリ領域が割り当てられており、各サービス・メモリ領域に対して適用可能な1以上のサービスが設けられている。本実施形態では、エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、アプリケーションに適用されるサービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。

【0050】

図4には、ICカード50のメモリ空間の基本構成を示している。図3を参照しながら既に説明したように、ICカード50内のメモリ空間に対して、「ディレクトリ」に類似する階層構造が導入され、所望の階層のエリアに、アプリケーションに割り当てられたサービス・メモリ領域を登録することができる。同図に示す例では、エリア0000定義ブロックで定義されるエリア0000内に、1つのサービス・メモリ領域が登録されている。

【0051】

図示のサービス・メモリ領域は、1以上のユーザ・ブロックで構成される。ユーザ・ブロックはアクセス動作が保証されているデータ最小単位のことである。

このサービス・メモリ領域に対しては、サービス 0108 定義ブロックで定義されている 1 つのサービスすなわちサービス 0108 が適用可能である。

【0052】

本実施形態では、エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、サービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。アクセス制限の対象となるサービスに関する暗証コード設定情報は、暗証コード専用のサービス（すなわち「暗証コード・サービス」）として定義される。

【0053】

図 4 に示す例では、サービス 0108 に関する暗証コードが暗証コード・サービス 0128 定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

【0054】

サービス 0108 に対する暗証コード・サービスが有効になっている場合、サービス 0108 を起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なう前に、暗証コード・サービス 0128 を使用した暗証コードの照合が必要となる。具体的には、暗号化あり読み書き (Read/Write) コマンドを使用する場合は、相互認証前にサービス 0108 に対する暗証コードの照合を行なう。（暗証コード・サービスを有効／無効にする仕組みについては後述に譲る。）

【0055】

また、本実施形態では、アプリケーションに割り当てられたサービス・メモリ領域を所望の階層のエリアに登録するとともに、エリアを階層化する（関連性の深いエリア同士を同じ親エリアに登録する）ことができる。この場合、エリア毎に暗証コードを設定することにより、エリアをアクセス制限の単位とすることができる。

【0056】

図 5 には、IC カード 50 のメモリ空間においてエリアが階層化されている様子を示している。同図に示す例では、エリア 0000 定義ブロックで定義されているエリア 0000 内に、エリア 1000 定義ブロックで定義されている別のエ



リア 1000 が登録されている。

【0057】

図 5 に示す例では、さらにエリア 1000 内には、2 つのサービス・メモリ領域が登録されている。一方のサービス・メモリ領域に対しては、サービス 1108 定義ブロックで定義されているサービス 1108 と、サービス 110B 定義ブロックで定義されているサービス 110B が適用可能である。このように、1 つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義することを、本明細書中では「オーバーラップ・サービス」と呼ぶ。オーバーラップ・サービスにおいては、同じサービス・エリアに対して、入力した暗証コードに応じて異なるサービスが適用されることになる。

【0058】

また、他方のサービス・メモリ領域に対しては、サービス 110C 定義ブロックで定義されているサービス 110C が適用可能である。

【0059】

各サービス・メモリ領域に設定されているサービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことができる。勿論、図 4 を参照しながら説明したように、サービス毎に暗証コード・サービスを定義することができる。この場合、サービスに対する暗証コード・サービスが有効になっているときには、暗証コード・サービスを使用した暗証コードの照合を行なってからサービスの起動が許可される。

【0060】

また、複数のサービスに対して共通の暗証コードを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。

【0061】

図 5 に示す例では、エリア 1000 に関する暗証コードが、暗証コード・サービス 1020 定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

【0062】

エリア1000に対する暗証コード・サービスが有効（後述）になっている場合、暗証コード・サービス1020を使用した暗証コードの照合を行なった後に、エリア1000内の各サービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことが可能となる。

【0063】

ここで、エリア1000内のサービスに暗証コード・サービスが適用されており且つこれが有効となっている場合には、さらにその暗証コード・サービスを使用した暗証コードの照合を経てからでないと、そのユーザ・ブロックに読み出し又は書き込み動作を行なうことはできない。

【0064】

図4及び図5に例示したように、暗証コード照合の対象となるエリアやサービスに対応する暗証コード・サービスは一意に与えられる。

【0065】

D. 暗証コード・サービスの登録

暗証コード・サービスのICカード50への登録は、通常のサービスと同様の登録サービス・コマンドを使用して行なう。

【0066】

但し、暗証コード・サービスの登録は、暗証コード照合の対象となるエリアやサービスが既にICカード50に登録済みであることが条件となる。すなわち、暗証コード照合の対象となるエリアやサービスがない場合は、暗証コード・サービスの登録サービス実行時にエラーとなる。

【0067】

また、暗証コード・サービスは、通常のサービスのユーザ・ブロックに相当する暗証コード・サービス・データ・ブロックが1ブロックしか存在しないので、サービス登録時に登録サービス・コマンドで指定ユーザ・ブロック数を1以外の値に設定するとエラーとなる。

【0068】

図6には、ICカード50内のメモリ空間にエリアやサービスを登録するための手順を示している。

【0069】

まず、メモリ空間にエリアが定義される（ステップS1）。

【0070】

次いで、サービスの登録サービス・コマンドを使用して、エリア内にアプリケーションに対してサービス・メモリ領域を割り当てるとともに、このサービス・メモリ領域に適用されるサービスを定義する（ステップS2）。登録サービス・コマンドでは、サービス・メモリ領域のユーザ・ブロック数を指定する。エリア内で複数のアプリケーションを割り当てたい場合には、当該処理ステップを繰り返し実行する。

【0071】

エリア内で定義したサービスに対して暗証コードを適用したい場合には、サービスの登録サービス・コマンドを使用して、暗証コード・サービスの登録を行なう（ステップS3）。

【0072】

さらに、エリア内で定義されたすべてのサービスに対して共通の暗証コードを設定したい場合には、サービスの登録サービス・コマンドを使用して、このエリアに対して共通の暗証コード・サービスの登録を行なう（ステップS4）。

【0073】

なお、ステップS3とステップS4の実行順序は逆であってもよい。

【0074】

さらに、1つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義したい場合には、サービスの登録サービス・コマンドを使用して、オーバーラップ・サービス（図5を参照のこと）を登録する（ステップS5）。

【0075】

そして、オーバーラップ・サービスに対して暗証コードを適用したい場合には、サービスの登録サービス・コマンドを使用して、暗証コード・サービスの登録を行なう（ステップS6）。

【0076】

図4に示した例では、ルートエリア0000内にサービス・メモリ領域の割

り当て並びにこれに適用するサービス 0108 が登録された後、サービス 0108 に適用される暗証コード・サービスが登録される。

【0077】

また、図 5 に示した例では、ルートのエリア 0000 下のエリア 1000 内で、2 つのサービス・メモリ領域が割り当てられるとともに、それぞれに適用されるサービス 1108、サービス 110C が登録される。また、一方のサービス・メモリには、他のサービス 110B がオーバーラップ・サービスとして登録される。図示しないが、これらに暗証コードを適用したい場合には、別途、暗証コード・サービスの登録が行なわれる。そして、登録されたサービス 1108、110B、110C に対して共通の暗証コードを設定したい場合には、エリア 1000 に対して共通の暗証コード・サービスを登録する。

【0078】

E. 暗証コードの適用

図 4 及び図 5 に例示したように、IC カード 50 内のメモリ空間に登録されたエリアやサービスに対して暗証コードを適用して、エリア単位、あるいはサービス単位でアクセス制御を行なうことができる。また、1 つのサービス・メモリ領域に対して複数のサービス（オーバーラップ・サービス）を登録することができるが、サービス毎に暗証コードを適用することで、同じサービス・メモリ領域に対して複数のアクセス方法を定義することができる。

【0079】

暗証コードの適用内容は、暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックに記述されている。図 7 には、暗証コード・サービス・データ・ブロックのデータ構造を模式的に示している。同図に示すように、暗証コード定義領域は、暗証番号領域と、入力失敗回数記憶領域と、最大許容入力失敗回数設定領域と、暗証番号使用選択領域と、アクセス許可フラグとで構成されている。

【0080】

ユーザが入力した暗証コードが一致した場合にのみ、該当するサービス又はエリアの暗証コード・サービス・データ・ブロック内のアクセス許可フラグを立て

て、其処へのアクセスを許可する。

【0081】

アクセス許可フラグは、該当するアプリケーション又はディレクトリのアクセス可否状態を示すためのフラグであり、アクセス許可フラグが設定されたサービス又はエリアはアクセス許可状態である。暗証コードが設定されたサービスやエリアのアクセス許可フラグは、デフォルトではアクセス不可状態であり、暗証コードの照合処理や秘密鍵を用いた認証処理に成功した後、アクセス許可フラグが設定されて、アクセス許可状態に転じる。また、アクセス許可フラグを設定し続けると、ICカード50又は携帯端末10が紛失した場合や盗難に遭った場合にサービスやエリアの無断使用・不正使用によりユーザが損害を被るおそれがある。このため、ICカード50は、例えばRF部51において電磁波が途絶えたことに応答してアクセス許可状態を自動的にアクセス不可にする機構を備えていてもよい。

【0082】

また、誤った暗証コードが入力された場合には、その都度、入力失敗回数記憶領域の記録を更新する。そして、入力失敗回数が最大許容入力失敗回数設定領域に設定された最大許容入力失敗回数に到達した場合には、該当するサービスの起動又はエリアに対するアクセスを禁止する。

【0083】

一般には、この入力失敗回数は、一度入力に成功したらクリアするべきものである。このようにして悪意あるユーザがしらみつぶしに暗証コードを調べることが防止する。また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、ICカード50を管理する管理者のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば後述するような秘密鍵による認証を使用することもできる。

【0084】

図8には、ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順をフローチャートの形式で示している。

【0085】

ユーザから暗証コードを入力すると（ステップS11）、照合部53は、各暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックにアクセスして、暗証コードが一致するか否かを判別する（ステップS12）。

【0086】

暗証コード・サービス・データ・ブロックの暗証コードがユーザ入力された暗証コードと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、対応するサービス又はエリアをアクセス可能状態にする（ステップS13）。

【0087】

暗証コードは、例えば、ICチップ50をリーダ／ライタ101にかざして、リーダ／ライタ101に接続されている外部機器（図示しない）のユーザ・インターフェースを用いて入力したものを、無線インターフェースすなわちRF部51経由でICチップに送信することができる。

【0088】

図8に示すように暗証コードを用いてアプリケーションやディレクトリへのアクセス権を制御する場合、悪意のあるユーザはしらみつぶしに暗証コードを調べることにより、セキュリティの壁が破られる可能性がある（特に桁数の少ない暗証コードを用いる場合）。このため、本実施形態では、暗証コード定義領域において、最大許容入力回数を設定して、入力失敗回数が最大許容入力回数に到達したアプリケーション又はディレクトリをアクセス不可状態に設定することで、アクセス制御を行なうようにしている。

【0089】

図9には、暗証コードの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順をフローチャートの形式で示している。

【0090】

ユーザから暗証コードを入力すると（ステップS21）、照合部53は、各暗証コード・サービス定義ブロックにアクセスして、暗証コードが一致するか否かを判別する（ステップS22）。

【 0 0 9 1 】

ユーザ入力された暗証コードが暗証コード・サービス定義ブロックの暗証コードと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、該当するサービス又はエリアをアクセス可能状態にする（ステップ S 2 3）。

【 0 0 9 2 】

他方、ユーザ入力された暗証コードがいずれの暗証コード・サービス定義ブロックの暗証コードとも一致しない場合には、暗証コード定義領域内の入力失敗回数を更新する（ステップ S 2 4）。また、ユーザ入力された暗証コードがいずれの暗証コード・サービス定義ブロックの暗証コードと一致し、照合に成功した場合には、入力失敗回数を 0 にクリアする。

【 0 0 9 3 】

そして、ステップ S 2 5 では、更新された入力失敗回数が、暗証コード定義領域内で設定されている最大許容入力回数に到達したか否かを判断する（ステップ S 2 5）。

【 0 0 9 4 】

もし、入力失敗回数が最大許容入力回数に到達してしまったならば、その暗証コード定義領域内のアクセス許可フラグの設定を解除して、該当するサービス又はエリアをアクセス不可状態にする（ステップ S 2 6）。この結果、悪意のあるユーザがしらみつぶしに暗証コードを調べる行為を取り締まることができる。

【 0 0 9 5 】

また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、I C カード 5 0 を管理する管理者のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば秘密鍵による認証を使用することもできる。

【 0 0 9 6 】**F. 暗証コード比較出力の制御**

既に述べたように、サービス又はエリアに対する暗証コード・サービスが有効になっている場合にのみ、サービスの起動又はエリアへのアクセスを行なう前に

、暗証コードの照合が要求され、暗証コード・サービスが無効にされている場合には、暗証コードの照合は要求されない。

【 0 0 9 7 】

この項では、暗証コード・サービスの有効／無効の設定による暗証コード比較出力の制御について説明する。

【 0 0 9 8 】

図 1 0 には、I C カード 5 0 における暗証コード比較出力の制御に関する機能構成を模式的に示している。

【 0 0 9 9 】

同図に示すように、I C カード 5 0 は、非接触・無線インターフェースなどからなる通信部 1 5 1 と、価値情報などのデータを保持するデータ保持部 1 5 2 と、データ保持部 1 5 2 へのアクセスを制御する暗証コードを保持する暗証コード保持部 1 5 3 と、通信部 1 5 1 から入力された暗証コードと暗証コード保持部 1 5 3 に保持されている暗証コードとを比較照合する暗証コード比較部 1 5 4 と、暗証コード比較を行なう条件に従って暗証コード比較出力を制御するフロー制御部 1 5 5 とを備えており、暗証コード識別装置を構成する。

【 0 1 0 0 】

通信部 1 5 1 では、図 1 1 に示すように、1 バイト単位にデータが送受信されるものとする。同図において、1 バイト・データの開始は、必ずスタート・ビットで開始するものとする。その後、8 ビット分のデータが続き、最後にストップ・ビットが来る。各ビット長は、固定で、送受信者間で事前に取り決めておくものとする。

【 0 1 0 1 】

また、図 1 2 には、1 バイト・データが集まって構成されるパケットの構成を模式的に示している。同図に示すように、パケットの前半はコード部であり、また、パケットの後半はデータ部（ペイロード）となっている。コード部には、そのパケットの意味付けを示すデータが記述されている。また、データ部は、コードに付随する何らかのデータ（データ本体）が必要な場合に添付されている。

【 0 1 0 2 】

また、図13には、送受信者間におけるパケット交換の基本シーケンスを示している。本実施形態においては、送信者を外部装置100とし、受信者を暗証コード識別装置としてのICカード50とする。

【0103】

パケットは、送信者から受信者へ何らかのアクションを要求するコマンドと、そのコマンドのアクションの結果として、受信者から送信者へ返送されるレスポンスに分けることができる。本実施形態で使用するコマンドとレスポンスを、以下の表に示しておく。

【0104】

【表1】

コマンド(外部装置→識別装置)		レスポンス(識別装置→外部装置)		意味
コード部	データ部	コード部	データ部	
10h	暗証コード	12h	OK/NG	暗証コード入力
18h	暗証コード	1Ah	OK/NG	暗証コード変更
20h	読み出し位置	22h	OK(読み出したデータ)/NG	データ読み出し
30h	書き込みデータ, 書き込み位置	32h	OK/NG	データ書き込み
40h	フラグ値	42h	OK/NG	有効/無効 変更
50h	フラグ値	52h	OK/NG	無効→有効 変更
60h	フラグ値	54h	OK/NG	有効→無効 変更

【0105】

コマンドのコード部10hは、データ部に設定した暗証コードを暗証コード識別装置としてのICカード50へ入力することを示す。通信部151によってコード部が解釈されると、引き続くデータ部が、暗証コード比較部54へ伝達されることになる。

【0106】

暗証コード比較部154は、伝達されたデータ部と暗証コード保持部153内に保持されている暗証コードとを比較し、一致している場合は、一致出力を出力する。そして、フロー制御部155は、データ保持部152と通信部151間でのデータ伝送を制限する機能を有する。

【0107】

図14には、フロー制御部155の構成を示している。

【0108】

有効／無効フラグ155Aは、データ保持部152と通信部151間の伝送路を接続状態とするか非接続状態とするかを、暗証コード比較部154の比較出力に応じて決定するかどうかを示すフラグである。

【0109】

有効／無効フラグ155Aが”1”で有効側のときには、スイッチ2は比較出力側となる。そして、暗証コード比較部154の出力が一致を出力している場合には、それがスイッチ1へ伝わってスイッチ1をオン状態とし、データ保持部152と通信部151の伝送路を接続状態とすることで、外部装置100が通信部151を介してデータ保持部152へのアクセスが可能となる。また、暗証コード比較部154の出力が不一致の場合には、それがスイッチ1へ伝わってスイッチ1をオフ状態とし、データ保持部152と通信部151の伝送路を非接続とすることで、外部装置100は通信部151を介してデータ保持部152にアクセスすることができない。

【0110】

他方、有効／無効フラグ155Aが”0”で無効側のときには、スイッチ2は常時オン側となる。したがって、暗証コード比較部154の比較出力によらず、スイッチ1を常時オン状態とし、データ保持部152と通信部151の伝送路の接続状態を維持する。

【0111】

この有効／無効フラグ155Aによって、暗証コード比較が不必要な場合には、その機能を抑制すなわち暗証コード・サービスを無効にすることが可能となるという点を充分理解されたい。

【0112】

無効→有効フラグ155Bは、コマンド・コード50hによって変更することができるフラグである。無効→有効フラグ155Bは、後述するコマンド・コード40hによって有効／無効フラグを、”0”の無効の状態から”1”の有効の

状態へ書き換えを行なう際に暗証コードの一致が必要かどうかを選択するためのフラグである。すなわち、無効→有効フラグが” 1 ” のときには本動作が成され、有効／無効フラグ 155A が” 0 ” で暗証コード比較が無効であって且つ比較出力が一致している場合には、スイッチ 3 をオンの状態にして、通信部 151 からの有効／無効フラグ 155A の書き換えを許可する。一方、無効→有効フラグが” 0 ” のときには、フラグ判別部 155D の出力部の出力は常にスイッチ 3 をオンの状態にして、通信部 151 からの有効／無効フラグ 155A の書き換えを常に許可する。

【0113】

無効→有効フラグ 155B が” 1 ” の場合には、有効／無効フラグ 155A を無効から有効に変更する際に暗証コードの一致が必要であることを示す。また、無効→有効フラグ 155B が” 0 ” の場合には、有効／無効フラグ 155A を無効から有効に変更する際に暗証コードの一致が不必要であることを示す。

【0114】

一方、有効→無効フラグ 155C は、コマンド・コード 60h によって変更することができるフラグである。有効→無効フラグ 155C は、後述するコマンドコード 40h によって有効／無効フラグ 155A を、” 1 ” の有効の状態から” 0 ” の無効の状態へ書き換えを行なう際に、暗証コードの一致が必要かどうかを選択するためのフラグである。すなわち、有効→無効フラグ 155C が” 1 ” のときに本動作が成され、有効／無効フラグ 155A が” 1 ” で暗証コード比較が有効であって且つ比較出力が一致している場合には、スイッチ 3 をオンの状態にして、通信部 151 からの有効／無効フラグ 155A の書き換えを許可する。一方、有効→無効フラグが” 0 ” のときには、フラグ判別部 155D の出力部の出力は常にスイッチ 3 を ON の状態にして、通信部 151 からの有効／無効フラグ 155A の書き換えを常に許可する。

【0115】

有効→無効フラグ 155C が” 1 ” の場合には、有効／無効フラグ 155A を有効から無効に変更する際に暗証コードの一致が必要であることを示す。また、有効→無効フラグ 155C が” 0 ” の場合には、有効／無効フラグ 155A を有

効から無効に変更する際に暗証コードの一致は不必要である。

【0116】

上述したような有効／無効フラグの変更制御オペレーションは、フラグ判別部 155D によって行なわれる。このオペレーションを論理的に整理すると、フラグ判別部 155D の出力は、以下の [表 2] に示す通りとなる。

【0117】

【表 2】

		有効／無効			
		1		0	
		比較出力		比較出力	
		一致	不一致	一致	不一致
無効→有効	1	0	0	1	0
	0	0	0	1	1
有効→無効	1	1	0	0	0
	0	1	1	0	0

【0118】

コマンド・コード 40h は、有効／無効フラグ 155A を変更するためのコマンドであり、上述した動作により、スイッチ 3 がオンの状態のときにのみ通信部 151 からの変更が可能である。

【0119】

このような仕組みにより、暗証コードを変更する際に、暗証コードを無効な状態から有効な状態にするには暗証コードを入力する必要はないが、逆に、暗証コードを有効な状態から無効な状態にするには暗証コードを入力する必要があるといったように、暗証コードの入力条件をさまざまに組み合わせて設定することが可能となる。

【0120】

以上説明したような処理オペレーションを経て、スイッチ 1 がオン状態になるとデータ保持部 152 と通信部 151 が接続状態となるため、それ以降は、リーダー／ライタ 101 側では、コマンド・コード 20h によってデータ保持部 152

内の所定位置からデータの読み出しを行ったり、コマンド・コード 30h によって所定データをデータ保持部 152 に書き込んだりすることが可能になる。

【0121】

暗証コード保持部 153 に既に書き込まれている暗証コードを書き換える際には、コマンド・コード 18h を使用する。書き換えが可能かどうかは、スイッチ 4 によって制御することが可能である。

【0122】

図 14 に示す例では、前述の無効→有効フラグ 155B、有効→無効フラグ 155C のそれぞれの状態、有効／無効フラグ 155A の状態、並びに、暗証コード比較部 154 の状態に応じて、フラグ判別部 155D によって制御するようになっている。すなわち、それぞれのフラグの状態に応じてスイッチ 4 の制御条件を変更することができ、例えば、無効→有効フラグ 155B が”0”から”1”にセットされる際に暗証コード保持部 153 の暗証コードを変更するようにすることも可能である。これによって、暗証コードの判別を有効にするときには、それ以前に設定されていた暗証コードに関係なく、新たな暗証コードを設定することが可能である。簡単なコマンド操作によって設定の書き換えを行なうことができるが、通信部 151 とリーダ／ライタ 101 との間に相互認証手段を挿入することで、セキュリティ・レベルを高めることも可能である。

【0123】

図 3～図 5 に示したように IC カード 50 内のメモリ領域が拡張されて、複数のアプリケーション（サービス・メモリ領域）が割り当てられている場合など、複数の暗証コードを用いてアクセス権を制御する場合においても、図 10 に示した暗証コード比較出力の仕組みを適用することができる。

【0124】

図 15 には、暗証コード保持部及び暗証コード比較部を複数個装備した暗証コード識別装置（IC カード 50）の構成例を示している。図 15 に示す例では、複数の暗証コード比較部 154 においてすべてが一致出力を出力したときにのみ、データ保持部 152 と通信部 151 が接続状態になるように構成する。これによって、暗証コードを入力する一部のリーダ／ライタ 101 を個人ユーザとする



とともに、暗証コードを入力する他の一部のリーダ／ライタ 101 を運用する運用者（例えば、当該カード・サービスの管理者など）に割り当てることにより、運用者側の判断によって、暗証コード機能を制御することが可能となる。例えば、利用者の意思に拘わらず、強制的に暗証コードの入力が必要なように設定することが可能となる。

【0125】

また、図 16 には、データ保持部 152 の個々のメモリ領域に対して暗証コードをそれぞれ設定できるようにした暗証コード識別装置（IC カード 50）の構成例を示している。

【0126】

暗証コード比較部 154 は、データ保持部 152 に割り当てられた各メモリ領域と暗証コードとの関係を示したルックアップ・テーブルを持っており、そのルックアップ・テーブルに従って、通信部 151 から入力された暗証コードが該当するメモリ領域の暗証コードと一致しているか否かを判別することができる。そして、互いの暗証コードが一致する場合には、該当するメモリ領域のアクセスを可能にする。以下の〔表 3〕には、暗証コード比較部 154 において管理されるルックアップ・テーブルの構成例を示している。

【0127】

【表 3】

暗証コード	許容メモリ開始アドレス	許容メモリ終了アドレス
暗証コード 1	100h	180h
暗証コード 2	300h	3A0h
暗証コード 3		
⋮	⋮	⋮

【0128】

このような構成によれば、通信部 151 を介して入力された暗証コードは、各



暗証コード比較部 154 において、ルックアップ・テーブル中に保持されているそれぞれの暗証コードと比較が行なわれる。そして、データ保持部 152 が持つメモリ空間のうち一致出力が得られた暗証コードに該当するメモリ領域に対するアクセスを許可するようにすることができる。

【0129】

[追補]

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈すべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0130】

【発明の効果】

以上詳記したように、本発明によれば、メモリ領域上に 1 以上のアプリケーションが割り当てられた情報記憶媒体において、アプリケーションに割り当てられている個々のサービス・メモリ領域に対して、ユーザ毎に異なるアクセス権限を与え、複数のアクセス方法を提供することができる、優れた情報記憶媒体及び情報記憶媒体のメモリ管理方法を提供することができる。

【0131】

本発明によれば、IC カード上のあるメモリ領域に対するアクセス権限が単一でない場合であっても、それぞれのアクセス権限に応じて暗証コードを個別に設定することができる。すなわち、同じサービス・メモリ領域について、適用すべきサービス毎に暗証コードが設定される。例えば、あるメモリ領域に対する読み出しについては暗証コードの入力が必要でないが、書き込む場合には暗証コードの入力を必須とさせることが可能である。

【図面の簡単な説明】

【図 1】

電磁誘導に基づくリーダー／ライター 101 と IC カード 50 との無線通信の仕組みを説明するための図である。

**【図 2】**

リーダ／ライタ 101 と IC カード 50 からなる系を 1 個のトランスとして捉えてモデル化した図である。

【図 3】

IC カード 50 内の機能構成を示した図である。

【図 4】

サービスに対して暗証コードを適用するための仕組みを説明するための図である。

【図 5】

エリアに対して暗証コードを適用するための仕組みを説明するための図である。

【図 6】

IC カード 50 内のメモリ空間にエリアやサービスを登録するための手順を示したフローチャートである。

【図 7】

暗証コード・サービス・データ・ブロックのデータ構造を模式的に示した図である。

【図 8】

ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順を示したフローチャートである。

【図 9】

暗証コードの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順を示したフローチャートである。

【図 10】

IC カード 50 における暗証コード比較出力の制御に関する機能構成を模式的に示した図である。

【図 11】

通信部 151 を介して 1 バイト単位で送受信されるデータの構造を模式的に示した図である。


【図 1 2】

1 バイト・データが集まって構成されるパケットの構成を模式的に示した図である。

【図 1 3】

送受信者間におけるパケット交換の基本シーケンスを示した図である。

【図 1 4】

フロー制御部 1 5 5 の構成を示した図である。

【図 1 5】

暗証コード保持部及び暗証コード比較部を複数個装備した暗証コード識別装置（ICカード 5 0）の構成例を示した図である。

【図 1 6】

データ保持部 5 2 の個々のメモリ領域に対して暗証コードをそれぞれ設定できるようにした暗証コード識別装置（ICカード 5 0）の構成例を示した図である。

【符号の説明】

5 0…ICチップ

5 1…RF部

5 2…メモリ

5 3…照合部

5 4…有線インターフェース

5 5…制御部

1 0 1…リーダ／ライタ

1 5 1…通信部

1 5 2…データ保持部

1 5 3…暗証コード保持部

1 5 4…暗証コード比較部

1 5 5…フロー制御部

1 5 5 A…有効／無効フラグ

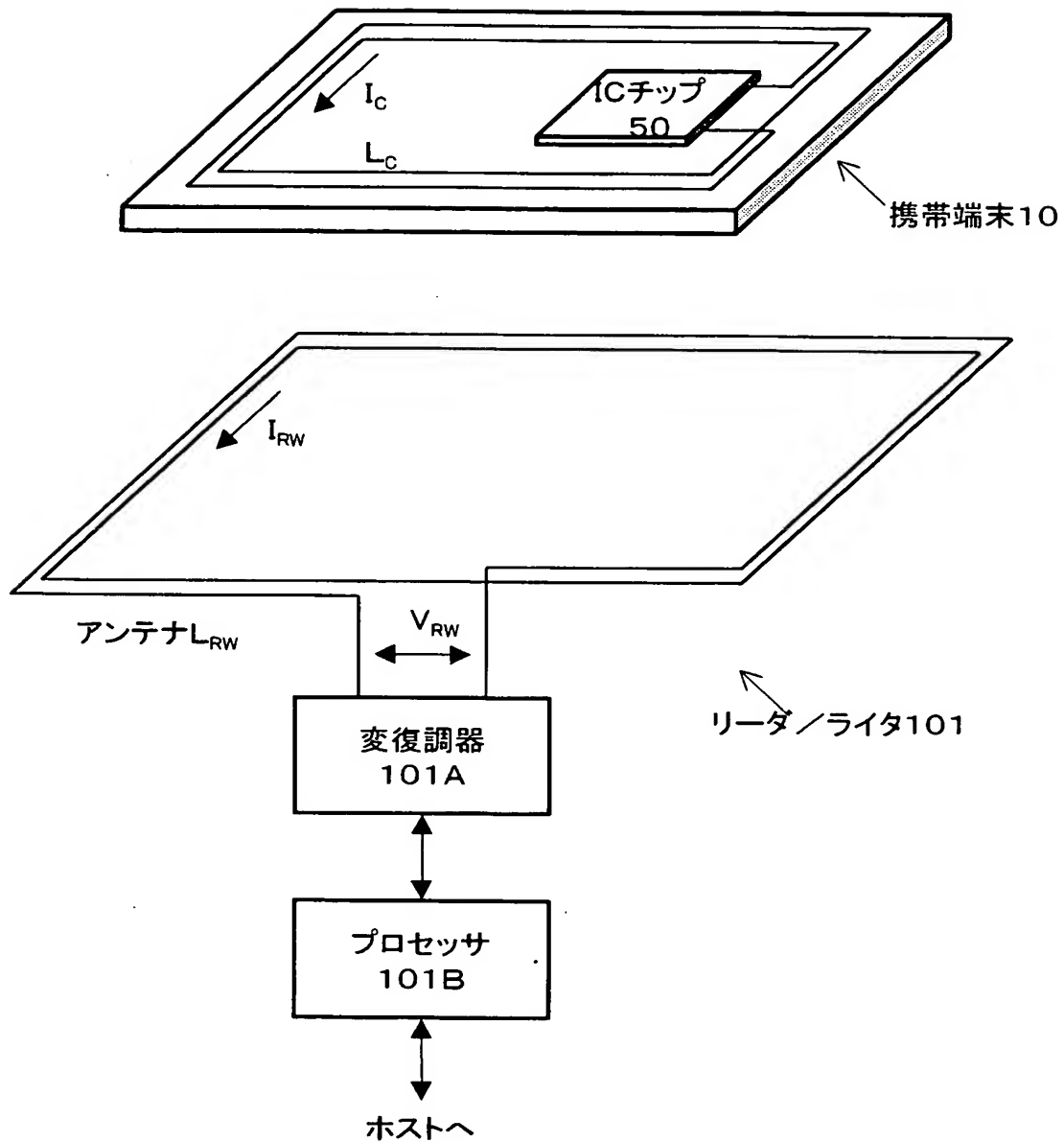
1 5 5 B…無効→有効フラグ

1 5 5 C…有効→無効フラグ

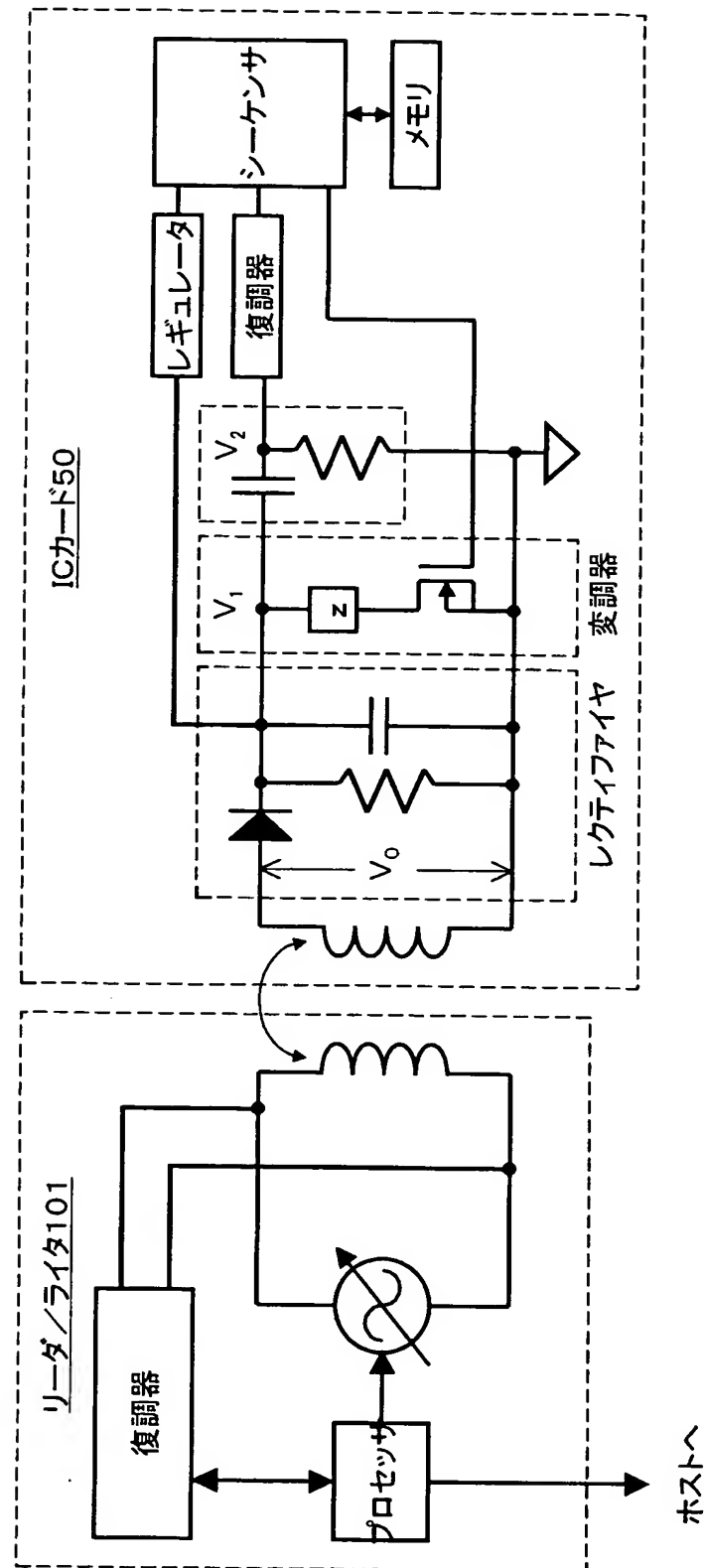
1 5 5 D…フラグ判別部

【書類名】 図面

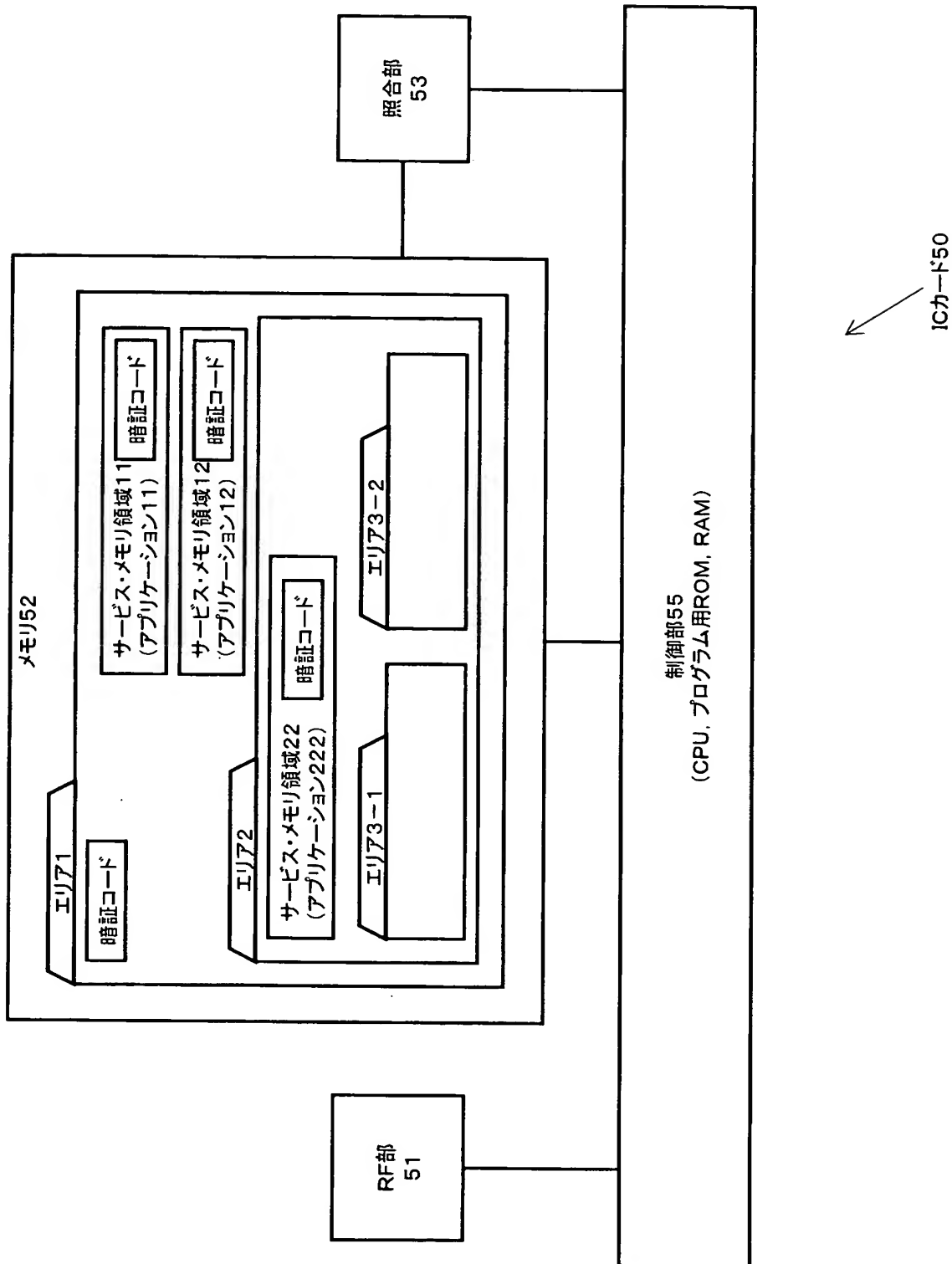
【図 1】



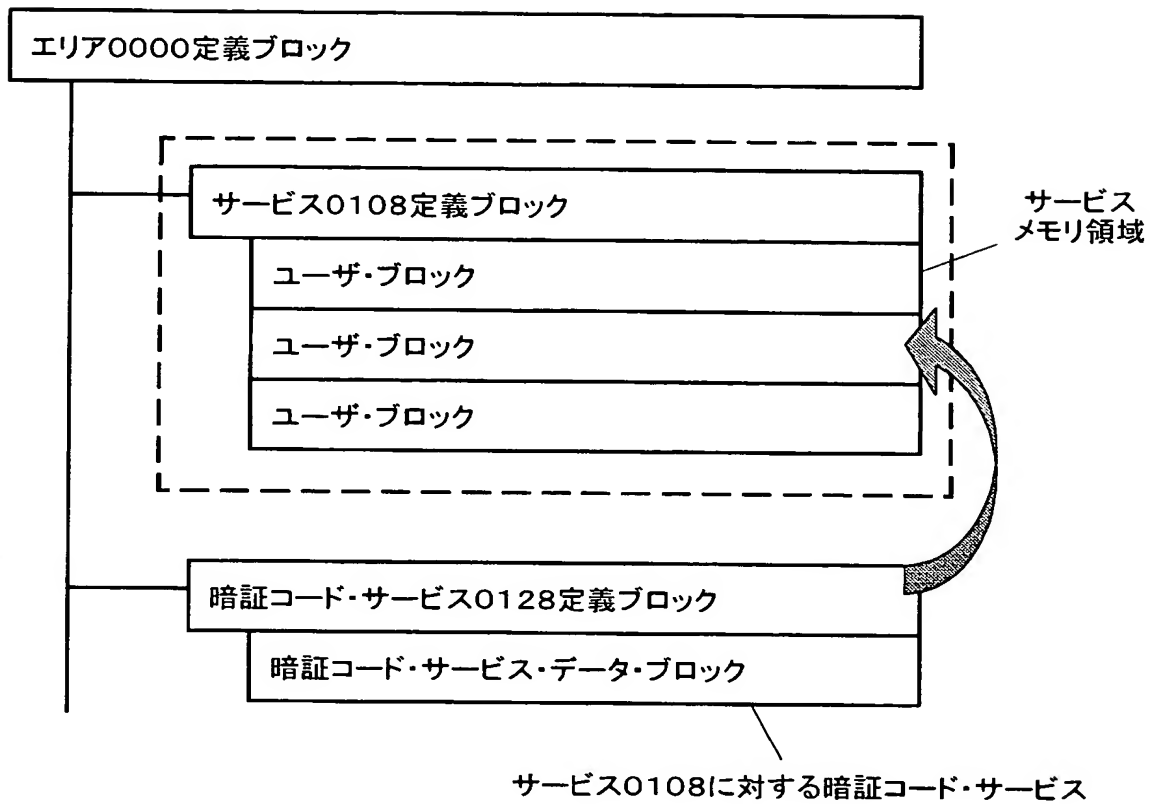
【図 2】



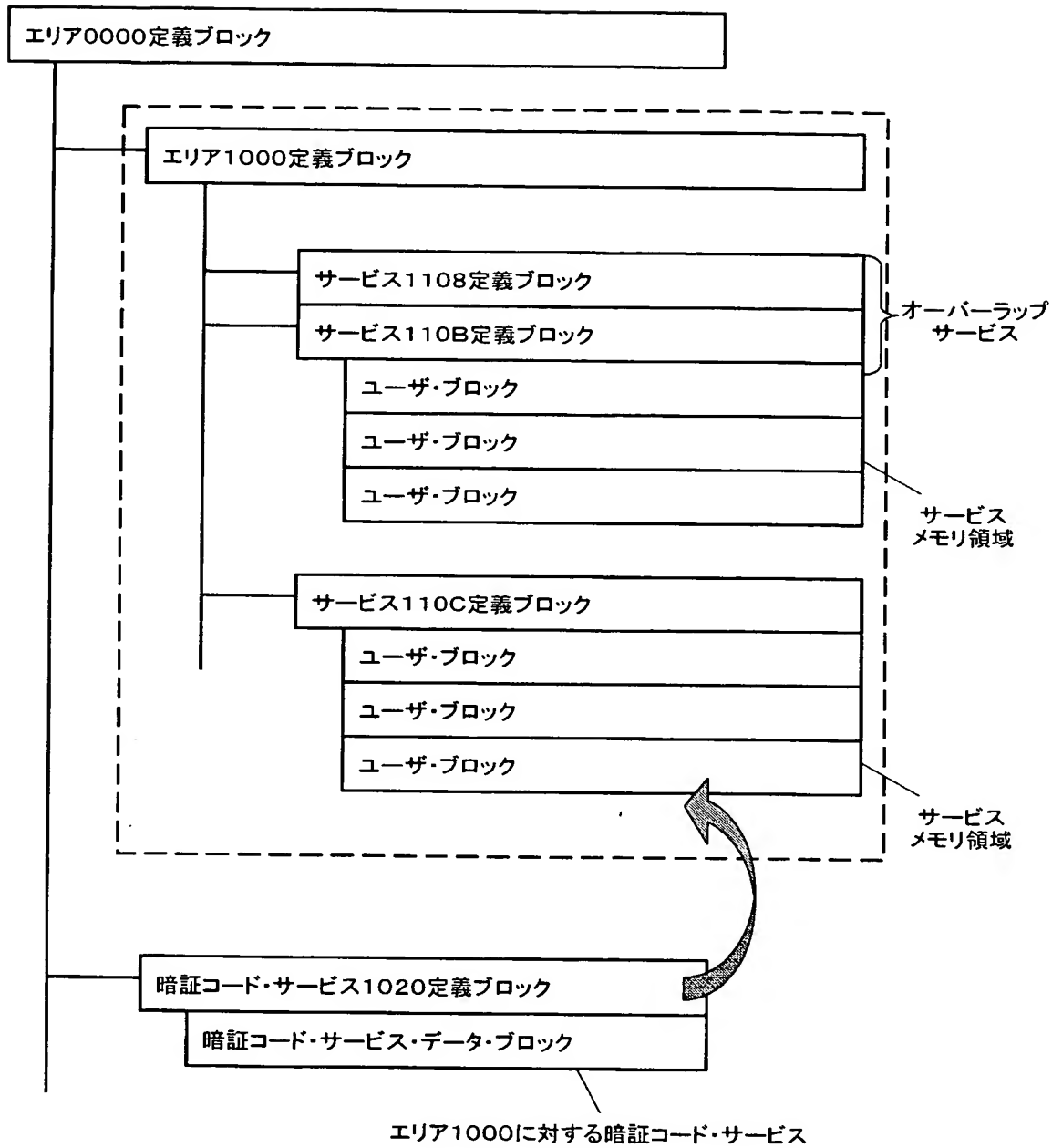
【図 3】



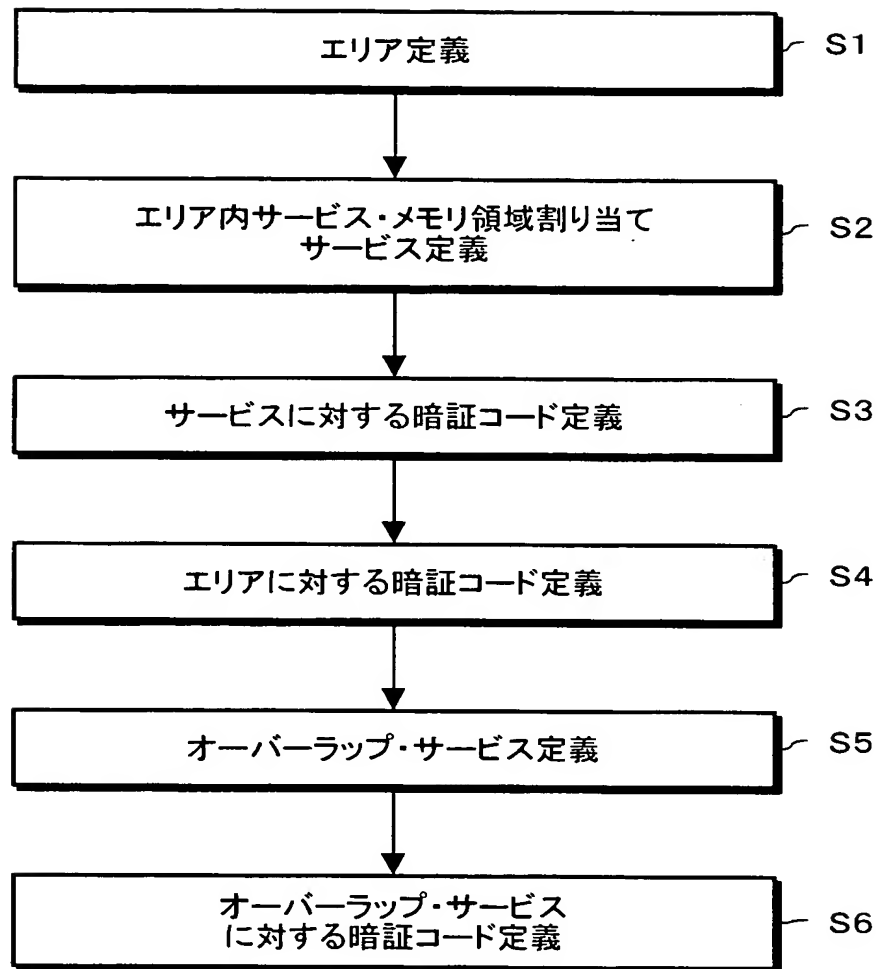
【図 4】



【図 5】



【図 6】



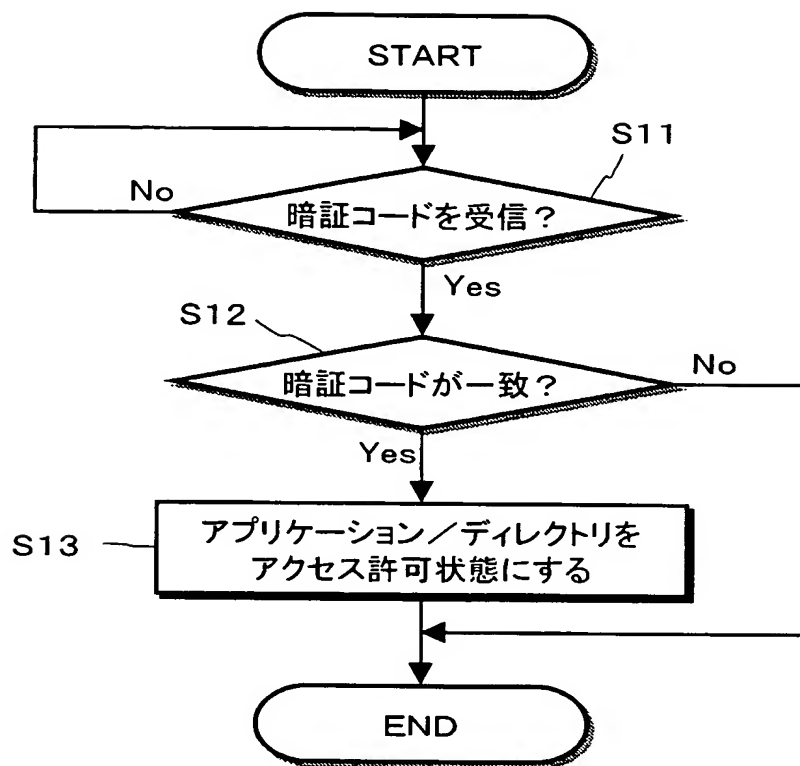
【図 7】

暗証コード 領域	入力失敗回数 記憶領域	最大許容入力失敗回数 設定領域	アクセス許可 フラグ
-------------	----------------	--------------------	---------------

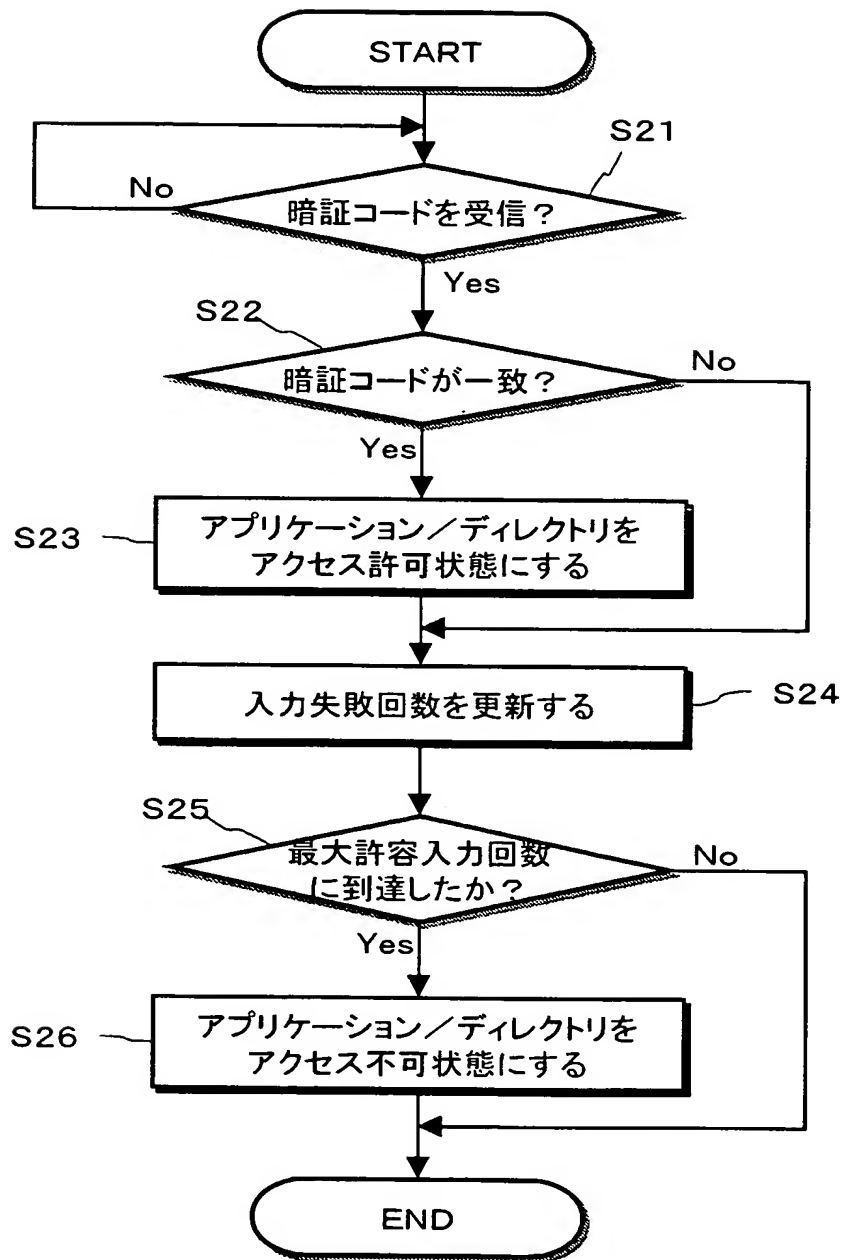
暗証コード・サービス・データ・ブロック



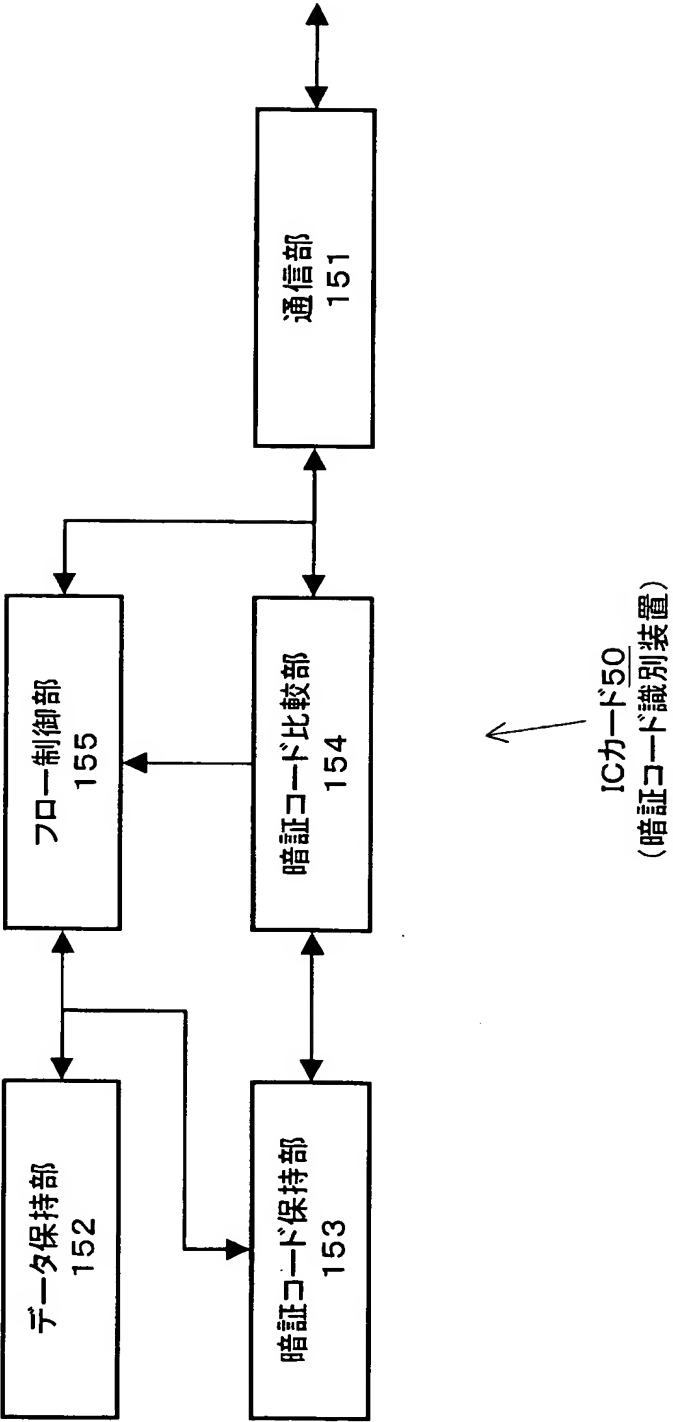
【図 8】



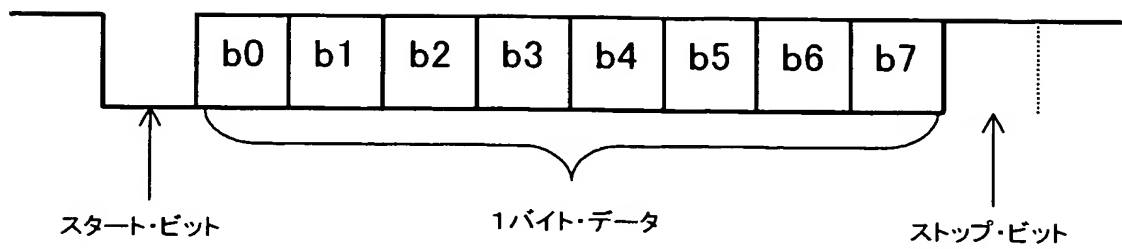
【図 9】



【図 10】



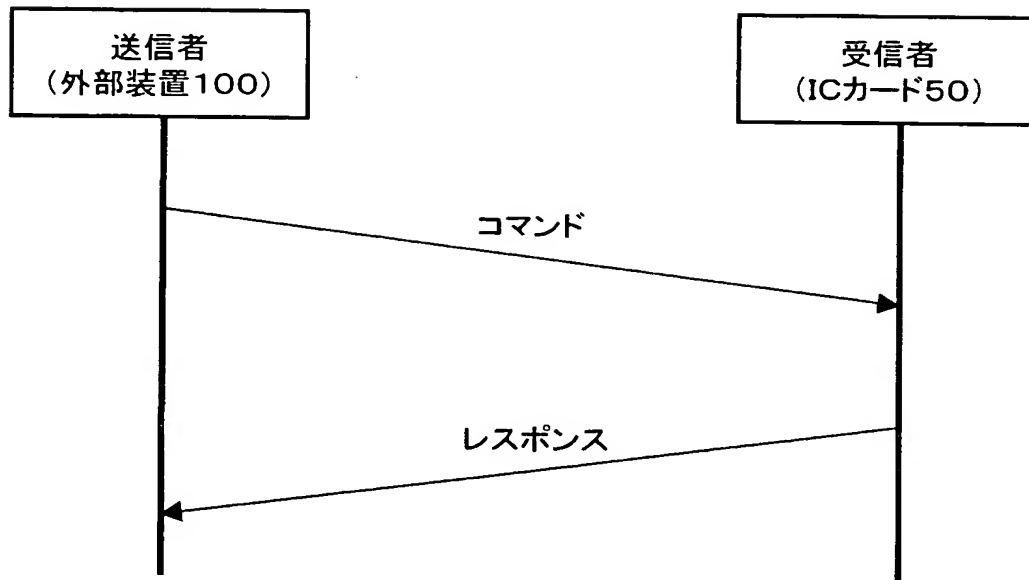
【図 1 1】



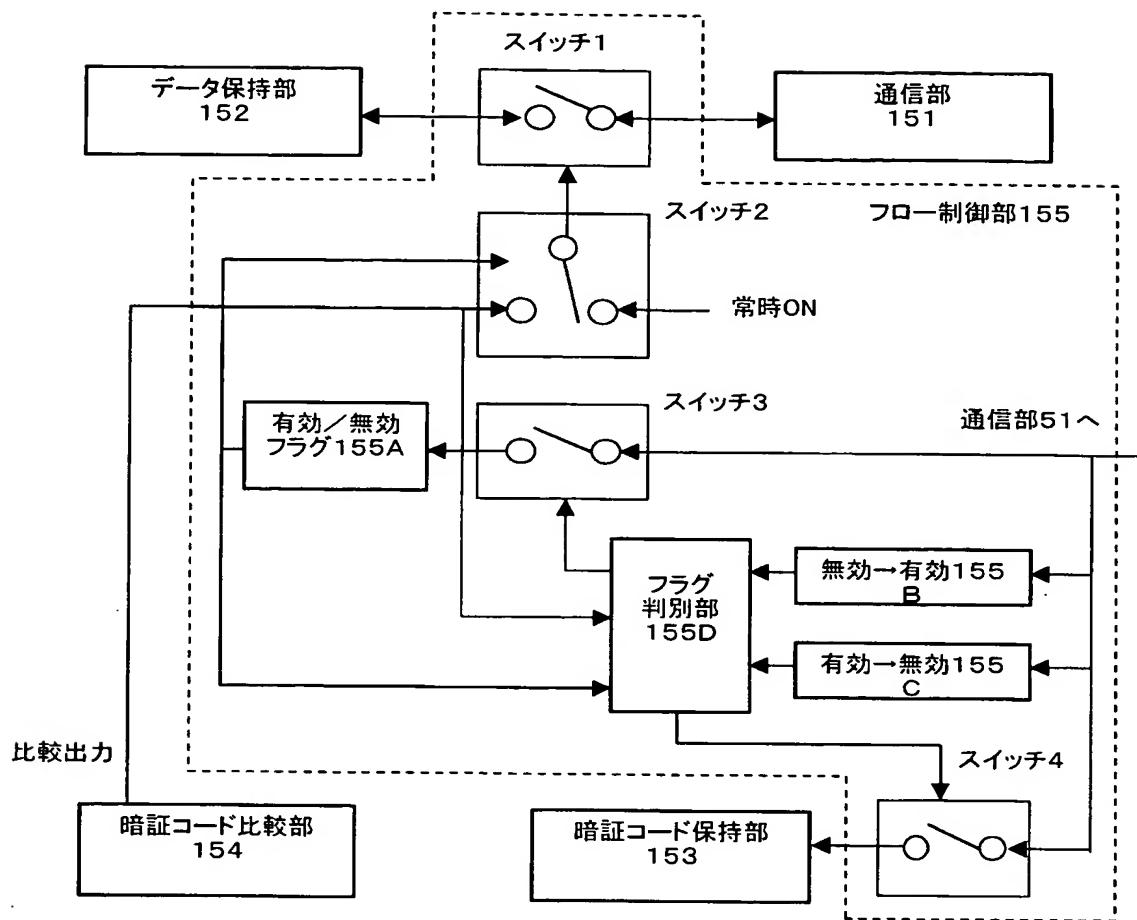
【図 1 2】



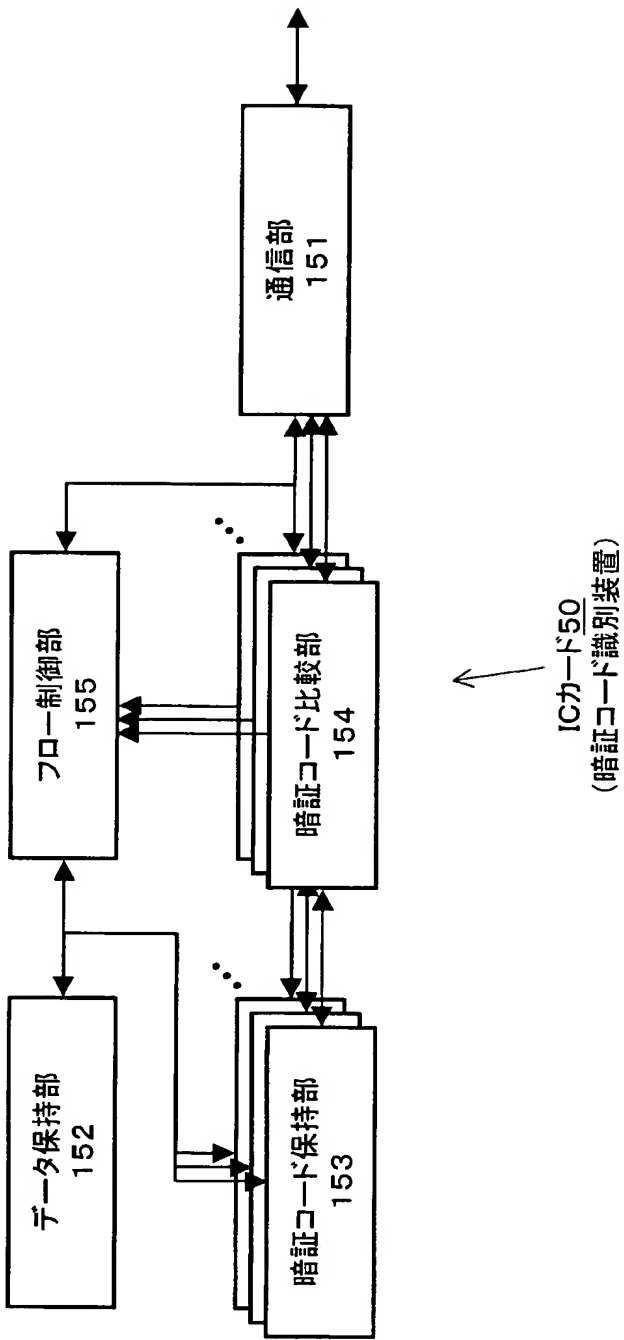
【図 13】



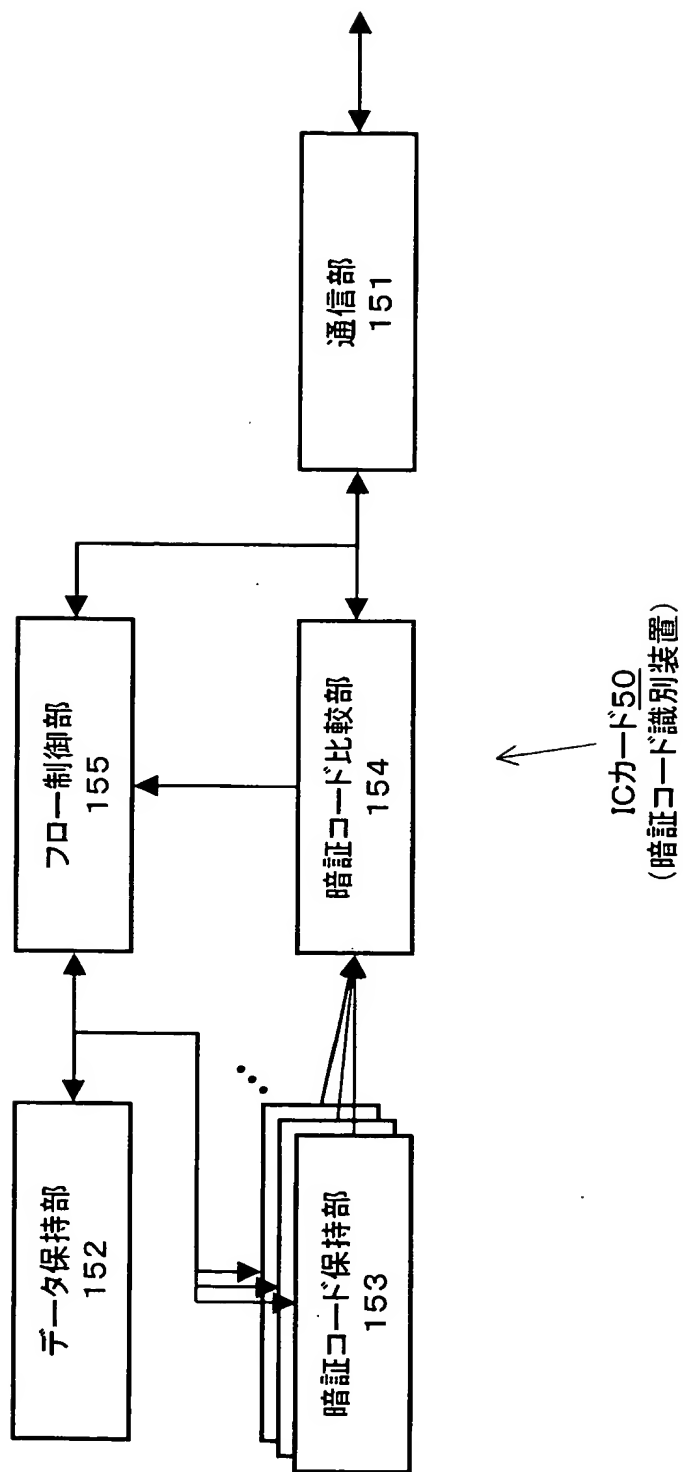
【図 14】



【図 15】



【図 16】




【書類名】 要約書

【要約】

【課題】 サービス・メモリ領域に対して複数のアクセス方法と、アクセス方法毎のアクセス権限を提供する。

【解決手段】 1つのサービス・メモリ領域に対して、複数サービスを重複して定義し（オーバーラップ・サービス）、サービス・メモリ領域に「読み出しのみ」、「読み出し及び書き込み」など複数のアクセス方法を設定する。オーバーラップ・サービス定義を行なう場合、サービス毎に暗証コードを設定するようにしてもよい。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定される。

【選択図】 図5



特願 2 0 0 3 - 1 0 4 7 0 6

ページ： 1/E

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 1 8 5]

1. 変更年月日	1 9 9 0 年 8 月 3 0 日
[変更理由]	新規登録
住 所	東京都品川区北品川 6 丁目 7 番 3 5 号
氏 名	ソニー株式会社